

09183739-110998

1 1. A method of network surveillance, comprising:  
2 receiving network packets handled by a network  
3 entity;

4 building at least one long-term and at least one  
5 short-term statistical profile from at least one measure of  
6 the network packets, the at least one measure monitoring  
7 data transfers, errors, or network connections;

8 comparing at least one long-term and at least one  
9 short-term statistical profile; and

10 determining whether the difference between the  
11 short-term statistical profile and the long-term statistical  
12 profile indicates suspicious network activity.

1 2. The method of claim 1, wherein the measure  
2 monitors data transfers by monitoring network packet data  
3 transfer commands.

1 3. The method of claim 1, wherein the measure  
2 monitors data transfers by monitoring network packet data  
3 transfer errors.

1 4. The method of claim 1, wherein the measure  
2 monitors data transfers by monitoring network packet data  
3 transfer volume.

1 5. The method of claim 1, wherein the measure  
2 monitors network connections by monitoring network  
3 connection requests.

1 6. The method of claim 1, wherein the measure  
2 monitors network connections by monitoring network  
3 connection denials.

1           7. The method of claim 1, wherein the measure  
2 monitors network connections by monitoring a correlation of  
3 network connections requests and network connection denials.

1           8. The method of claim 1, wherein the measure  
2 monitors errors by monitoring error codes included in a  
3 network packet.

1           9. The method of claim 8, wherein an error code  
2 comprises a privilege error code.

1           10. The method of claim 8, wherein an error code  
2 comprises an error code indicating a reason a packet was  
3 rejected.

1           11. The method of claim 1, further comprising  
2 responding based on the determining whether the difference  
3 between the short-term statistical profile and the long-term  
4 statistical profile indicates suspicious network activity.

1           12. The method of claim 11, wherein responding  
2 comprises transmitting an event record to a network monitor.

1           13. The method of claim 12, wherein transmitting  
2 the event record to a network monitor comprises transmitting  
3 the event record to a hierarchically higher network monitor.

1           14. The method of claim 13, wherein transmitting  
2 the event record to a network monitor comprises transmitting  
3 the event record to a network monitor that receives event  
4 records from multiple network monitors.

1           15. The method of claim 14, wherein the monitor  
2 that receives event records from multiple network monitors  
3 comprises a network monitor that correlates activity in the  
4 multiple network monitors based on the received event  
5 records.

1           16. The method of claim 11, wherein responding  
2 comprises altering analysis of the network packets.

1           17. The method of claim 11, wherein responding  
2 comprises severing a communication channel.

1           18. The method of claim 1, wherein the network  
2 packets comprise TCP/IP packets.

1           19. The method of claim 1, wherein the network  
2 entity comprises a gateway, a router, or a proxy server.

1           20. The method of claim 1, wherein the network  
2 entity comprises a virtual private network entity.

1           21. A method of network surveillance, comprising:  
2 monitoring network packets handled by a network  
3 entity;  
4 building a long-term and multiple short-term  
5 statistical profiles of the network packets;  
6 comparing one of the multiple short-term statistical  
7 profiles with the long-term statistical profile; and  
8 determining whether the difference between the one  
9 of the multiple short-term statistical profiles and the  
10 long-term statistical profile indicates suspicious network  
11 activity.

09183739 " 1109998

1           22. The method of claim 21, wherein the multiple  
2 short-term statistical profiles comprise profiles that  
3 monitor different anonymous FTP sessions.

1           23. The method of claim 21, wherein building  
2 multiple short-term statistical profiles comprises  
3 deinterleaving packets to identify a short-term statistical  
4 profile.

1           24. A computer program product, disposed on a  
2 computer readable medium, the product including instructions  
3 for causing a processor to:  
4           receive network packets handled by a network entity;  
5           build at least one long-term and at least one short-  
6 term statistical profile from at least one measure of the  
7 network packets, the measure monitoring data transfers,  
8 errors, or network connections;  
9           compare at least one short-term and at least one  
10 long-term statistical profile; and  
11           determine whether the difference between the short-  
12 term statistical profile and the long-term statistical  
13 profile indicates suspicious network activity.

1           25. A method of network surveillance, comprising:  
2           receiving packets at a virtual private network  
3 entity; and  
4           building at least one long-term and at least one  
5 short-term statistical profile based on the received  
6 packets, and  
7           comparing at least one long-term statistical profile  
8 with at least one short-term statistical profile to  
9 determine whether the packets indicate suspicious network  
10 activity.

1           26. The method of claim ~~25~~, further comprising  
2 decrypting the packets before statistically analyzing the  
3 packets.

1           27. The method of claim ~~25~~, further comprising not  
2 decrypting the packets before statistically analyzing the  
3 packets.

09102739-11098  
SECRET